IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 09/934,184 §
Filed: August 21, 2001 §
Inventor: §
Sadler, et al. §
Title: MESSAGE §
MANAGEMENT §
SYSTEMS AND METHOD §

Examiner: Hewitt II, Calvin L
Group/Art Unit: 3621
Atty. Dkt. No: 5181-77301

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date indicated below.

Rory D. Rankin
Name of Registered Representative

Signature — November 3, 2006 Date

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request. This request is being filed with a notice of appeal. Applicant notes this is the second Request for Review in the present application, the first having resulted in the re-opening of prosecution. The review is requested for the reason(s) stated below.

Applicant is in receipt of the Advisory Action mailed October 4, 2006. Claims 1-14, 17-36, and 38-45 remain pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks.

Claims 1-6, 11, 15-20, 26-29, 33-42, 44, and 45 stand rejected under 35 U.S.C. § 102(b) as being anticipated U.S. Patent No. 5,005,200 (hereinafter "Fischer"); claim 7 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer in view of U.S. Patent No. 6,102, 287 (hereinafter "Maytas"); and claims 12-14, 30-32, and 43 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fischer. Finally, claims 21-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fisher in view of U.S. Patent No. 5,970,475 (hereinafter "Barnes"). Applicant submits the claims recite features neither disclosed nor suggested by the cited art. The following clear errors in the Examiner's rejection are noted.

Generally speaking, the claimed invention is directed to a system and method that a recipient may use to certify a message received from a sender whose identity may be

unknown to some degree. While the sender may include a digital signature in the message, the recipient may need to follow a process for certifying the message including verifying the signature before processing the message. Certification may also include routing the message to one or more external services that assist in the certification process. The recipient performs signature verification after the message is received, i.e., at a time when the message is no longer under the control or possession of the sender. More specific aspects of message routing are recited in the claims. For example, claim 1 recites:

> "A method for routing messages comprising:
> receiving a message from a sender;
>
> converting the message into an internal format, wherein said converting comprises adding at least an attribute part to a data part of the message;
> writing into said attribute part data extracted from said received message and data indicative of a protocol by which the message was received; and
> routing said converted message in dependence on the data in said attribute part."

Applicant submits claim 1 recites features that are neither disclosed nor suggested by the cited art. For example, in paragraph 7 of the Office Action, it is stated:

> "Fischer teaches a method for routing messages comprising:
>
> - receiving a message from a sender (column 17, lines 18-33)
> - a parser for converting the message into an internal format by adding at least an attribute part to a data part of the received message (column 17, lines 30-41 and 60-66)
> - a protocol handler for writing into said attribute part data extracted from said received message and data indicative of a protocol (column 17, lines 36-38 and 45-46)
> - routing said converted message in dependence on the data in said attribute part (figure 5; column 11, lines 25-52; column 12, lines 55-62; column 17, lines 26-30; column/line 17/60-18/2; column 19, lines 1-6)
>
> . . ."

It is first noted that the above excerpt from the Final Office Action is not an entirely accurate representation of what is actually recited in the claims. For example, claim 1 recites the features "writing into said attribute part data extracted from said received message and data indicative of a protocol by which the message was received." In the above excerpt, the examiner represents the claim(s) as reciting "writing into said attribute part data extracted from said received message and data indicative of a protocol." As can be seen, this representation is not equivalent to that which is recited. Applicant has reviewed Fischer and finds no disclosure of "writing into said attribute part data extracted from said received message and data indicative of a protocol by which the message was received." For at least this reason, each of the independent claims are patentably distinguishable from the cited art. Further, not only does Fischer not disclose or suggest the recited features, but Fischer discloses nothing at all regarding protocols by which a message is received, or protocols generally. The examiner cites column 17, lines 36-38 and 45-46 of Fisher as disclosing the

above recited features. However, Applicant can find no such teaching included therein. Such features are also not disclosed in Maytas or Barnes.

In view of the above, Applicant submits each of the independent claims, and all of the claims, are patentably distinguishable from the cited art for at least the above reasons, and the rejections should be withdrawn.

In addition to the above, Fischer merely discloses a method of validating a received message that includes examining each of a set of included signatures to validate that they are certified. For example, Fischer discloses:

> "In validating the object and its signatures, the recipient may, for example proceed as follows.
>
> . . .
>
> the owner of 154 has obtained the necessary counter signatures 160 and 164 by the holders of certificates 162 and 166, as well as the necessary joint-signatures 168, 180 and 200.
>
> . . .
>
> All certificates must be accompanied by signatures which are themselves authorized by antecedent certificates. Ultimately all the authority can be traced to a set of certificates which have been signed by the holder of the meta-certificate (or possibly a small set of meta-certificates). Each meta-certificate is well known and distributed to all parties "throughout the world".
>
> The recipient examines every signature supplied and verifies that each accurately signs its purported object (whether the object is a primary object, a certificate, or another signature) using the procedure detailed in FIG. 3. The recipient insures that each signature includes a corresponding validated certificate.
>
> If a certificate requires joint signatures, then the recipient insures that the required number of these necessary signatures (to the same object) are present. If the certificate requires counter signatures, then the recipient insures that the required number from the designated subset are present (the counter signatures have signatures as their object).
>
> All certificates are then examined. A check is made for the special meta-certificate which has no signature but which is universally known and trusted and a copy of which is already stored in the recipient's computer. If a certificate is received which claims to be the meta-certificate but which is not equal to that already known to and accepted by the recipient, then a rejection is issued. If the meta-certificate is properly recognized, then the validation process continues." (Fischer, col. 21, line 45 to col. 22, line 46).

As may be seen from the above, the recipient examines every signature supplied and verifies that validating certificates accompany each one. All required signatures and corresponding certificates must be present in the message for it to be validated. It is up to the owner (sender) to obtain the necessary counter signatures and joint-signatures. While, Fischer may therefore disclose receiving a message from a sender, Fischer does not disclose writing data extracted from said received message and data indicative of a protocol by which the message was received into said attribute part, or routing said converted message in

dependence on the data in said attribute part, as recited. Rather, Fischer's validation method merely includes an examination of the signatures and certificates included in the message.

Generally speaking, the portions of Fischer cited by the Examiner describe procedures for a message owner to obtain necessary counter signatures and joint-signatures before sending the message, rather than a method for routing a message received from a sender. For example, Fischer discloses:

> "Turning next to the creation of a counter signature which is shown in FIG. 4, initially A signs at 63 a primary object 60 in accordance with the procedure . . .. The primary object 60 may be a purchase order or some other commitment or it may be a counter signature of some other signature of a primary object.
>
> . . . the process of A signing an object may also involve some other party signing A's signature. Thus, A's certificate 62 specifically defines at 65 that, in order for A's signature to be valid (i.e., ratified), a counter signature by C is required, for example, using C's specific certificate Y.
>
> After A signs the object, A's signature packet 66 is then forwarded along with the primary object and all associated signatures and certificates to C and A requests that C add his counter signature 64. Upon receiving the material, C reviews all existing signature certificates and the primary object and if everything meets with his approval he would decide to sign A's signature 68. A's signature inherently reflects the primary object and C's signature inherently reflects A's signature so C will essentially have "signed on the line below A's signature".
>
> Once C decides to approve A's signature at 68, the process of creating a signature . . . is duplicated except that the object is A's signature. Thus, with A's signature as the object (and the type of object being designated as a signature at 72), the counter signature date 74, C's counter signature comment 76, and C's certificate 70 are applied to a hashing algorithm 80 to thereby result in a presignature hash 82. At the same time, these fields are also inserted into the counter signature packet 88 as discussed above with respect to the signature packet 42 (with a hashing algorithm 69 being applied to the signature object).
>
> Presignature hash 82 and C's secret key 92 are applied in a signature operation 84 to generate a counter signature seal 86. This counter signature seal becomes part of the counter signature packet 88 in precisely the same fashion as described previously in regard to the creation of signature packet 42 in FIG. 2.
>
> Because the certificate "Y" which C must use to perform the signature has been explicitly stated (in the certificate which A used to sign), C may also be required to meet his own cosignature obligations so specified by "Y" and forward this entire package including his own newly added signature on to other parties for further cosignatures (either joint or counter signatures). This recursive signature gathering process continues until sufficient signatures are added to fully satisfy all cosignature requirements of at least one party who initially signed the primary object." (Fischer, col. 17, line 18 to Col. 18, line 2).

Therefore, Fischer discloses that A forwards a signature packet along with the primary object and all associated signatures and certificates to C. Upon receiving the material, C reviews all existing signature certificates and the primary object and if everything meets with his approval he may decide to sign A's signature. Using a broad interpretation of claim 1, one might equate A's forwarding a primary object with signatures to C with C receiving a message from a sender. However, Fischer does not disclose that C converts a message into an internal format, as recited. Rather, C merely reviews all existing signature certificates and the primary object and if everything meets with his approval, signs A's signature. Signing A's signature is not equivalent to the recited adding an attribute part to a data part and "writing into said attribute part data extracted from said received message and data indicative of a protocol." Furthermore, Fischer does not disclose routing said converted message in dependence on the data in said attribute part, as recited. C merely forwards the entire package to other parties for further cosignatures. However, since C's forwarding is based on data that existed in the primary object and was not added to an attribute part, C's forwarding is not dependent on data in the attribute part.

For at least these additional reasons, Applicant submits that claim 1 is patentably distinguishable over the cited art, taken either singly or in combination.

In light of the foregoing remarks, Applicant submits the application is in condition for allowance, and notice to that effect is respectfully requested. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicant hereby petitions for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5181-77301/RDR.

Respectfully submitted,

Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: November 3, 2006